

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA

v.

VINCENT J. FUMO,
Defendant.

:
:
:
:
:
:
:
:

CRIMINAL ACTION

NO. 06-319

Memorandum and Order

YOHN, J.

October ___, 2007

Presently before the court is defendant Vincent J. Fumo's motion to compel production of information pertaining to the government's search of computer files and digital media, presumably brought pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E). Fumo seeks the information to determine whether the government's searches and seizures violated his Fourth Amendment rights. Because the requested information is not material to application of the exclusionary rule, this motion will be denied.

I. Background

Fumo was charged in connection with four categories of wrongdoing in a superseding indictment issued on February 6, 2007: (1) fraud and conspiracy to commit fraud on the Senate of Pennsylvania ("Senate"); (2) fraud and conspiracy to commit fraud, conspiracy to obstruct the Internal Revenue Service, and aiding and assisting in the filing of false tax returns related to Citizens Alliance for Better Neighborhoods ("Citizens Alliance"); (3) fraud on the Independence

Seaport Museum; and (4) obstruction of justice and conspiracy to obstruct justice. Pursuant to the government's investigation of the various schemes to defraud and to obstruct justice, federal agents examined computer equipment that was (1) voluntarily provided by witnesses, (2) obtained by grand jury subpoena, and (3) seized pursuant to search warrants. (Gov't Mem. 3.)

Pursuant to its investigation of obstruction of justice and fraud on Citizens Alliance, the government applied for and obtained warrants to search Fumo's Philadelphia district office and the home of Leonard Luchko, a Senate computer aide and codefendant in this case. On February 18, 2005, federal agents searched Fumo's district office pursuant to a warrant issued by United States Magistrate Judge M. Faith Angell. (Case No. 05-M-197.) This warrant permitted seizure of computer equipment containing, inter alia, emails relating to grand jury subpoenas received by Citizens Alliance and relating to an email from Luchko instructing employees to delete emails to and from Fumo. The warrant also authorized seizure of the relevant emails found on the computer equipment, as well as emails that were deleted in response to the Luchko email.

On October 20, 2005, pursuant to a warrant issued by United States Magistrate Judge Carol Sandra Moore Wells, federal agents searched Luchko's home. (Case No. 05-M-1078.) The warrant permitted seizure of computer equipment containing, inter alia, emails concerning subpoenas and search warrants received by Fumo, his staff, and Citizens Alliance, and documents relating to any efforts by Fumo and his staff to destroy records relevant to the federal investigation. Again, the warrant also authorized seizure of the relevant documents and emails.

As the investigation expanded from obstruction of justice and fraud on Citizens Alliance to include additional crimes, the government applied for a third search warrant. On January 31, 2007, the government sought from United States Magistrate Judge Charles B. Smith a warrant to

search all of the computer evidence previously obtained by subpoena and the search warrants for evidence pertaining to all the schemes detailed in the superseding indictment. (Case No. 06-M-116.) The warrant was issued, permitting seizure of documents and emails relating to (1) “work or services provided by any Senate of Pennsylvania employer or contractor” for the personal or political benefit of Fumo, his family, and his personal friends; (2) work performed by specified Senate contractors; (3) Fumo’s “acquisition or use of any property of the Independence Seaport Museum for his personal benefit”; and (4) “the identities of Senate employees, or friends, family members, or associates of Fumo, who were given cell phones or other communications equipment for which the Senate or Citizens Alliance paid.”

In sum, then, the three warrants permitted seizure of computer equipment and emails and other documents found on the equipment that related to the schemes to defraud the Senate, Citizens Alliance, and the Independence Seaport museum, as well as documents and emails that related to the scheme to obstruct justice.

On June 28, 2007, counsel for Fumo sent a letter to the Assistant United States Attorney prosecuting this action, formalizing a request for “additional discovery relating to the forensic analysis of all computer media in this case.” (Def.’s Mem. Ex. A, at 1.) Specifically, Fumo sought twelve categories of documents and computer files:

(1) All documents reflecting, relating or referring to any search protocols and procedures employed by the government in connection with the government’s forensic examination of all digital media in this matter, including but not limited to all servers, PCs, hard drives, PCMCIA cards, DVDs, CDs, diskettes, BlackBerry devices, cellular phones, and compact flash or secure digital cards seized by the government pursuant to those warrants (the “Digital Media”);

(2) All files and documents identifying the keywords or phrases used by the government in connection with each search of each specimen of Digital

Media, including but not limited to the keywords referenced in the June 28, 2006 Form 302 report of FE Donald Justin Price at page 11 and in his May 2, 2005 Form 302 report at page 3;

(3) All audit logs and case reports generated by the “Forensic Toolkit” software (“FTK”), as identified in the June 28, 2006 Form 302 report of FE Price at page 9, and in his May 2, 2005 Form 302 report at page 2, together with logs or reports generated by any similar software used in connection with the government’s forensic examination of each specimen of Digital Media;

(4) All files and documents reflecting the “bookmarks” created by the government’s forensic examiners for the purpose of identifying specific files for the government’s further review, as identified in FE Price’s June 28, 2006 Form 302 report at page 11 and in his May 2, 2005 Form 302 Report at page 3;

(5) All “examination notes” and other “administrative documents” as identified in FE Price’s June 28, 2006 Form 302 report at page 11 and in his May 2, 2005 Form 302 report at page 3;

(6) All examination results, as originally copied to CD-ROMs, as identified in FE Price’s June 28, 2006 Form 302 report at page 11 and in his May 2, 2005 Form 302 report at page 3;

(7) All files or documents reflecting the results of searches or investigations intended to obtain evidence of alleged wiping of electronically stored information or the use of key-logging or antikey logging software;

(8) All files reflecting the “derivative evidence” including but not limited to the evidence identified as “DEPH13,” at page 2 of FE Price’s May 2, 2005 Form 302 report and the evidence identified as “DEPH 1” through “[]DEPH 23,” at pages 9 and 10 of FE Price’s June 28, 2006 Form 302 report;

(9) All files incorporating or reflecting any FTK custom filters developed in connection with the government’s forensic examination of each specimen of Digital Media;

(10) All files or documents reflecting the government’s use or attempted use of password recovery software, including but not limited to DataAccess’s software packages known as “Password Recovery Toolkit” and “Distributed Network Attack”;

(11) All Microsoft Access databases or reports generated or produced in connection with the government’s forensic examination of each specimen of

Digital Media, as identified in FE Price's June 28, 2006 Form 302 report at page 11 and in his May 2, 2005 Form 302 report at page 3.

(12) All documents referring or relating to restrictions placed upon any government agent concerning the review of any electronic evidence to ensure conformance with all applicable legal privileges, Department of Justice policies relating to search and seizure of electronic evidence, and/or conformance with any prior agreement amongst counsel concerning the production of electronic evidence, including specifically, review of PCMCIA cards produced by the defendant.

(*Id.* at 1-2.)

On July 13, 2007, the government responded by letter, enclosing “[d]igital evidence worksheets and case notes prepared by Forensic Examiner D. Justin Price and Special Agent James P. McDonald” and “[a] CD containing Access databases that reflect file listings for electronic evidence obtained in the course of the investigation and email communications between FE Price and representatives of PGP concerning PGP software.”¹ (Def.’s Mem. Ex. B, at 1.) The government, however, “object[ed] to providing [Fumo] with the actual keyword terms that [were] used to search the computers that were seized.” (*Id.*) The government asserted that “the law is clear that the warrant need not specify how the computers will be searched,” that “there is absolutely no requirement that the government use keyword searches at all, much less identify the keywords it uses,” and that the “keyword terms that were used constitute confidential attorney work product.” (*Id.* at 3.)

In response, on July 20, 2007, Fumo filed the instant motion to compel production. As his memorandum of law in support of his motion deals only with the propriety of compelling the government to produce its search protocols and keywords (i.e., the information in requests 1 and

¹ Although not explicitly stated, these categories of documents appear responsive to requests 5 and 11.

2), I will confine the discussion to those issues.²

II. Standard

Discovery in criminal cases is governed by Federal Rule of Criminal Procedure 16. Rule 16(a)(1)(E),³ the portion of the rule most relevant here, states:

Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:

- (i) the item is material to preparing the defense;
- (ii) the government intends to use the item in its case-in-chief at trial; or
- (iii) the item was obtained from or belongs to the defendant.

Clearly subsection (iii) does not apply. Furthermore, neither party has suggested that the government intends to use the requested information in its case-in-chief at trial, so subsection (ii) does not apply. The relevant provision, then, is subsection (E)(i), and the question is whether the items sought are "material" to preparing the defense.

The defendant must make a prima facie showing of materiality. *United States v. RMI Co.*, 599 F.2d 1183, 1188 (3d. Cir. 1979). "Materiality means more than that the evidence in question bears some abstract logical relationship to the issues in the case. . . . There must be some indication that the pretrial disclosure of the disputed evidence would have enabled the

² In addition to arguing that the search protocols and keywords are legally irrelevant, the government argues that disclosure "would be prejudicial to the government. It would inappropriately reveal the methods, work product, and thought processes of government prosecutors and investigators." (Gov't Mem. 2.) Because the parties have not briefed the work product issue, and because I resolve the motion on other grounds, I will not consider whether work product protection applies to the search protocols and keywords.

³ Before 2002, the content of Rule 16(a)(1)(E) was included in Rule 16(a)(1)(C).

defendant significantly to alter the quantum of proof in his favor.” *Id.* (quoting *United States v. Ross*, 511 F.2d 757, 762-63 (5th Cir. 1975) and citing *United States v. Brown*, 562 F.2d 1144, 1152 n.8 (9th Cir. 1977); *United States v. Johnson*, 577 F.2d 1304, 1309 (5th Cir. 1978); *United States v. Orzechowski*, 547 F.2d 978, 984-85 (7th Cir. 1976)).

Information is not material when it is irrelevant to an asserted defense. For example, evidence supporting a defense is not material when the asserted defense is not, in fact, a defense to the crimes charged. *See United States v. Hsu*, 155 F.3d 189, 204 (3d Cir. 1998) (concluding that trade secrets in requested documents “are not ‘material’ to the preparation of the defendants’ impossibility defense” because legal impossibility is not a defense to the crimes charged); *see also United States v. Buckley*, 586 F.2d 498, 506 (5th Cir. 1978) (finding that “the information sought, by [defendant’s] own admission, related only [to] his entrapment defense, which, as we have already decided, was not ‘a defense’ in this case”). Likewise, in this case, the information sought is not material if it is irrelevant to the question whether evidence should be suppressed in accordance with the exclusionary rule.

Fumo requests the search protocols and keywords to determine whether the government, in searching the computer equipment and seizing documents and emails, violated the Fourth Amendment. He argues:

To apply the Fourth Amendment, a defendant must know the nature of the search conducted. In the digital world, that means a defendant must know the search protocols—and in particular any key words used by the government—in conducting its search. Senator Fumo carefully tailored a limited number of requests that, if answered, should at least begin to permit him to analyze whether the searches conducted comport with the Fourth Amendment.

(Def.’s Mem. 6-7.) More specifically, Fumo argues that the information requested is necessary

(and, I assume, material) because the question whether “the government’s search . . . strayed beyond the scope of the warrants at issue, or w[as] otherwise unreasonable in [its] scope, cannot be answered in the utter vacuum of information in which the government has left Senator Fumo.” (Def.’s Mem. 6.) The government argues in reply, however, that “any incorrect use of keywords is legally irrelevant,” and even if the search were overbroad, “the correct remedy would be suppression only of the particular items which were improperly reviewed.” (Gov’t Mem. 10.)

III. Search Protocols and Keywords Are Legally Irrelevant to the Suppression Remedy for Violations of the Fourth Amendment

The Fourth Amendment to the United States Constitution protects against unreasonable searches and seizures:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

When a defendant’s Fourth Amendment rights have been violated by a search or seizure of his property, “the principal means today for effectuating the rights secured by the Fourth Amendment is through the judicially created exclusionary rule.” *United States v. Christine*, 687 F.2d 749, 757 (3d Cir. 1982). If a seizure pursuant to a warrant is overbroad, the appropriate remedy is exclusion from use at trial of evidence outside the scope of the warrant. *Id.* This suppression remedy is available under Rule 12(b)(3)(C), which lists “motion to suppress” as one of five types of pretrial motions. To facilitate the making of this motion, Rule 12(b)(4) allows the government, “[a]t the arraignment or as soon afterward as practicable” to “notify the

defendant of its intent to use specified evidence at trial.”⁴ Thus, if Fumo later discovers that evidence offered by the government is beyond the scope of the items described in the warrants, he should file a motion to suppress individual exhibits.

The search protocols and keywords used by the government are irrelevant to the decision whether the warrants were overbroad or the seizures exceeded the scope of the warrants. In both cases, the constitutionality of the warrants and of the seizures of particular documents can be determined by examining only the warrants and the evidence.⁵

Individual documents offered into evidence might be subject to suppression because (1) the warrants allowing the seizures were overbroad, or (2) the seizure exceeded the scope of the warrants. First, if evidence offered by the government for admission at trial is the result of seizure pursuant to an overbroad warrant, overbreadth can be determined from the face of the warrant, and no further discovery is necessary. *See, e.g., Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 960 (3d Cir. 1984) (referring only to the inclusive language in a warrant authorizing a search a law office to determine that the warrant was overbroad). The warrant can be evaluated and, if necessary, redacted; evidence seized pursuant to the offending portions of the warrant can be excluded. *Christine*, 687 F.2d at 758 (“Materials seized under the authority of those parts of the warrant struck for invalidity must be suppressed, but the court need not suppress materials seized pursuant to the valid portions of the warrant.”). No information about

⁴ The government notes that it has “complied with [Rule 12(b)(4)] by producing all documentary evidence to the defense, and in the near future, on a schedule set by the Court, will further specify the exhibits it intends to offer at trial.” (Gov’t Mem. 9.)

⁵ Fumo does not argue that the warrants permitting the searches and seizures were in any way deficient, so I assume, when necessary, that they were not.

search protocols or keywords is necessary or relevant to the analysis.

Second, if the seizure exceeded the scope of the warrant, this will be apparent when the evidence offered is compared to the description on the face of the warrant of items to be seized and when defense counsel questions the proponent of the evidence about the circumstances of its seizure. *Cf. United States v. Coleman*, 805 F.2d 474, 483 (3d Cir. 1986) (noting that “[t]o the extent material outside the list [contained in the warrant] was seized, the district court properly determined that that material could be suppressed”). Again, information about search protocols or keywords is unnecessary and immaterial to the determination. Therefore, I will deny Fumo’s motion to compel.

The decision whether to suppress a document offered as evidence in this case will depend only on the connection between the document and the descriptions of documents to be seized listed in the warrants. Therefore, the broader context of the search is not relevant to Fumo’s defense.⁶ Because the parties briefed the issue of the relevance of search protocols and keywords to the constitutionality of the search, however, I will address it.

Regardless of the search protocols or keywords used by the government, the government may open and briefly examine each computer file to determine whether it is within the description recited in the warrant. The Supreme Court has been clear that a search need not be conducted in the least intrusive manner. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995). For example, in a search of a file cabinet, the government may examine briefly many

⁶ The exclusionary rule applies only when illegally seized evidence is offered for admission at trial. If a search or seizure was unconstitutional, but evidence obtained as a result of the illegality is not offered at trial, the available remedy is a suit against the officers as described in *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

documents in the course of looking for a particular document: “In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.” *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). The Third Circuit expanded on this observation, adding that “no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision.” *Christine*, 687 F.2d at 761. Instead, “flexibility is especially appropriate in cases involving complex schemes spanning many years that can be uncovered only by exacting scrutiny of intricate financial records.” *Id.* These rules are particularly applicable in the case of documents on computers, where files may be disguised, relevant documents may be intermingled with irrelevant ones, and “there is no way to know what is in a file without examining its contents.” *United States v. Hill*, 459 F.3d 966, 978 & n.14 (9th Cir. 2006); *see also United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *35-38 (S.D.N.Y. Apr. 4, 2007). For these reasons, search protocols and keywords do not mark the outer bounds of a lawful search; to the contrary, because of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant.

In support of his argument that “forensic investigators are not permitted to randomly peruse computer data simply because they have lawfully seized digital media” (Def.’s Mem. 5), Fumo cites *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999). In *Carey*, a computer technician and detective searching computer files for evidence of drug sales happened upon one image of child pornography in the course of their search. *Id.* at 1270-71. The Tenth Circuit held that they exceeded the scope of the warrant when they abandoned the original search and began looking for other pornographic images, *id.* at 1276, noting that the file cabinet analogy was

“inadequate” and “inapposite,” *id.* at 1275. The court, however, limited its holding to the facts of the case. *See id.* at 1276 (“[W]e are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.”). Additionally, the Tenth Circuit has narrowly construed the holding of *Carey* to be the truism that “law enforcement may not expand the scope of a search beyond its original justification.” *United States v. Grimmet*, 439 F.3d 1263, 1268 (10th Cir. 2006). Evidence seized must simply be “consistent with the probable cause originally articulated by the . . . judge.” *Id.* at 1268-69. As noted above, this comparison may be performed without reference to search protocols and keywords.

Fumo also relies on *In re Search of 3817 W. West End, First Floor*, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004), in which a magistrate judge determined that he had the power to require delineation of the government’s search protocol in the warrant, in order to ensure that a search of a home computer would not exceed the bounds of the Fourth Amendment. Fumo relies on the portion of the case in which the magistrate judge follows *Carey*, finding the file cabinet analogy “inadequate for purposes of the Fourth Amendment issue presented here.” *Id.* at 959 n.3. I am not persuaded by the Illinois district court’s use of *Carey*, however, given that the issue in this case, as Fumo acknowledges, is not whether the government must disclose its search protocols or keywords in advance (Def.’s Mem. 5), and that *Carey*’s holding was reined in by its own circuit.

For the reasons set out above, there is no requirement that the government, in executing a warrant, limit itself to its search protocols or keywords, so long as the search and seizure actually conducted are supported by the probable cause and within the scope of the particular descriptions recited in the warrants. Because deviations from search protocols and keywords are permissible,

knowledge of those protocols and keywords will not allow Fumo or a court to draw conclusions about the reasonableness of the search actually conducted. If the evidence is within the scope of the warrant, it will be admissible. If it is not, it will be suppressed unless an exception to the warrant requirement applies.

IV. Conclusion

The burden is on the defendant to make a prima facie showing of materiality pursuant to a motion to compel. Fumo has not made this showing. I agree with the government that its search protocols and keywords are not “material” for purposes of Rule 16(a)(1)(E). I will thus deny Fumo’s motion to compel production of information pertaining to the government’s search of computer files and digital media.

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA

v.

VINCENT J. FUMO,
Defendant.

:
:
: CRIMINAL ACTION
:
: NO. 06-319
:
:
:

Order

YOHN, J.

And now, this ____ day of October 2007, upon careful consideration of defendant Vincent J. Fumo's motion to compel production of documents and electronically stored information pertaining to the government's search of computer files and digital media (Docket No. 141) and the government's response thereto, IT IS HEREBY ORDERED that the motion is DENIED.

s/ William H. Yohn Jr.
William H. Yohn Jr., Judge